

NORMALIZED COCYCLES FOR LATIN QUANDLES

MARCO BONATTO

ABSTRACT. In the paper we will develop a combinatorial approach to the study of quandle coverings as defined in [3].

In the paper of Eisermann there is a complete categorical characterization of connected coverings of a given quandle X , but it involves the construction of the adjoint group of X , which is not easy to do and it has been computed just in some particular cases.

The quandle structure of a covering (Y, f) of a connected quandle X can be described by a cocycles which is a map $\beta : X \times X \rightarrow S^S$ (where S is a set of size equal to the size of the blocks of $\ker(f)$) satisfying some further condition. The same construction can be carried on in a more general setting and it works whenever the blocks of the congruence relative to a surjective morphism of binary algebras have all the same size and the properties of the map β depends on which kind of algebra you are dealing with.

Different cocycles can describe isomorphic coverings, then it is enough to study a proper quotient of the set of the cocycle (see [1]).

We will prove that for latin quandle there exists a special representative of any class of cocycles and using this particular features we will show that some classes of latin quandle have no proper coverings.

1. BASICS AND DEFINITIONS

For a set X , denote by $\text{Sym}(X)$ the set of all bijections $X \rightarrow X$ and by 1 the identity map over S .

For a groupoid (X, \cdot) and $x \in X$, let

$$L_x : X \rightarrow X, \quad L_x(y) = x \cdot y$$

be the *left multiplication* by x , and

$$R_x : X \rightarrow X, \quad R_x(y) = y \cdot x$$

the *right multiplication* by x .

For a groupoid (X, \cdot) , let $\text{Aut}(X)$ be the automorphism group of (X, \cdot) .

Definition 1.1. *A groupoid (X, \cdot) is a (left) rack if for $L_x \in \text{Aut}(X)$ for every $x \in X$. Equivalently, a groupoid (X, \cdot) is rack if it satisfies the left-distributive law*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$$

and $L_x \in \text{Sym}(X)$ for every $x \in X$.

A rack (X, \cdot) is faithful if the mapping $L : X \rightarrow \text{Aut}(X)$, $x \mapsto L_x$ is injective. A rack (X, \cdot) is latin if $R_x \in \text{Sym}(X)$ for every $x \in X$.

2000 *Mathematics Subject Classification.* Primary 05C38, 15A15; Secondary 05A15, 15A18.

Key words and phrases. Quandles, Coverings, Non Abelian Cohomology.

This paper is in final form and no version of it will be submitted for publication elsewhere.

Definition 1.2. A quandle is an idempotent rack, that is, a rack satisfying the idempotent law

$$x \cdot x = x.$$

Definition 1.3. The left multiplication group of a rack (X, \cdot) is the permutation group

$$\text{LMlt}(X) = \langle L_x : x \in X \rangle.$$

The group

$$\text{Trans}(X) = \langle L_x L_y^{-1} : x, y \in X \rangle$$

is the transvection group of (X, \cdot) .

Note that $\text{Trans}(X) \leq \text{LMlt}(X) \leq \text{Aut}(X)$.

Definition 1.4. A rack (X, \cdot) is homogeneous if $\text{Aut}(X)$ acts transitively on X , connected if $\text{LMlt}(X)$ acts transitively on X , and 2-connected if $\text{LMlt}(X)$ acts 2-transitively on X .

Lemma 1.5. Let X be a quandle and α its congruence. Then the mapping

$$\pi_\alpha^* : \text{LMlt}(Q) \longrightarrow \text{LMlt}(Q/\alpha), \quad L_{x_1} \dots L_{x_n} \mapsto L_{[x_1]} \dots L_{[x_n]}$$

is well defined and is a surjective homomorphism of groups.

Proof. This map is well defined since, if $L_{x_1} \dots L_{x_n} = L_{x'_1} \dots L_{x'_m}$, then

$$[L_{x_1} \dots L_{x_n}(y)] = [L_{x'_1} \dots L_{x'_m}(y)]$$

$$L_{[x_1]} \dots L_{[x_n]}[y] = L_{[x'_1]} \dots L_{[x'_m]}[y]$$

for every $[y] \in Q/\alpha$. By definition it follows that it is also a surjective group morphism. \square

The following classes of quandles will be used throughout the paper.

- Example 1.6.** (1) The one element set is called the trivial quandle;
 (2) Any projection algebra on a set X , which is a pair (X, \cdot) where $L_x = \text{id}_X$ for every $x \in X$, is a quandle, called the projection quandle over X ;
 (3) Let G be a group and $H \subseteq G$ a subset closed under conjugation. For $x, y \in H$, let $x \cdot y = xyx^{-1}$. Then $(H, \cdot) = \text{Conj}(H)$ is a quandle, the conjugation quandle on H ;
 (4) Let (X, \cdot) be a rack and $L_X = \{L_x : x \in X\}$ the set of all left multiplications of X . Note that L_X is closed under conjugation in $\text{LMlt}(X)$ since $L_x L_y L_x^{-1} = L_{x \cdot y}$. We obtain the quandle $L(X) = \text{Conj}(L_X)$;
 (5) Let G be a group, $\alpha \in \text{Aut}(G)$ and $H \leq \text{Fix}(\alpha) = \{x \in G : \alpha(x) = x\}$. Let G/H be the set of left cosets $\{xH : x \in G\}$ and define multiplication on G/H by

$$xH \cdot yH = x\alpha(x^{-1}y)H.$$

Then $(G/H, \cdot) = \mathcal{Q}(G, H, \alpha)$ is a quandle, called a coset or Galkin quandle. By [5, Theorem 7.1], a quandle is homogeneous if and only if it is isomorphic to some coset quandle $\mathcal{Q}(G, H, \alpha)$;

- (6) A coset quandle $\mathcal{Q}(G, H, \alpha)$ is called principal if $H = \{1\}$ and affine if G is Abelian;
 (7) Let X be a quandle and $L_x^2 = \text{id}_X$ for every $x \in X$, then X is called involutory.

Let us give a definition of covering equivalent to ([3, Definition 1.4]) using congruences.

Definition 1.7. *Let X, Y be quandles and $f : Y \rightarrow X$ be a surjective morphism. If the blocks of $\text{Ker}(f)$ have all the same size then f is called projection. If $\text{ker}(f) \leq \text{ker}(L)$ then the pair (Y, f) is said to be a covering of X .*

Every surjective quandle morphism between connected quandles is a projection, so this is not a restrictive assumption.

Proposition 1.8. *Let X be a quandle and α its congruence. If X/α is connected then all blocks of α have the same size.*

Proof. Let $[x], [y] \in X/\alpha$, then there exists $h \in \text{LMlt}(X/\alpha)$ such that $[y] = h([x])$. By Lemma 1.5 there exists $h' \in \text{LMlt}(X)$ such that $h = \pi^*(h')$ and

$$[h'(z)] = h([z])$$

for every $z \in X$. So h' maps the $[x]$ to the block $[h(x)] = [y]$, and its restriction to the block $[x]$ is bijective. \square

Every quandle is a covering. By definition we have

Fact 1. *Let X be a connected quandle, then (X, L) is a covering of $L(X)$.*

2. QUANDLE COVERINGS

In this section we summarize some well know results on quandle coverings, and the link between them and quandle cohomology. Most of the results can be found in [1] and can be extended to a more general class of binary algebras, but this is not the purpose of the paper, so we will stick to the quandle setting.

Definition 2.1. ([1, Definition 2.2]) *Let X be a quandle and S be a non-empty set. A map α :*

$$\beta : X \times X \rightarrow \text{Sym}(S)$$

is called a cocycle if it satisfies the following conditions

$$(C) \quad \beta(xy, xz)\beta(x, z) = \beta(x, yz)\beta(y, z)$$

$$(Q) \quad \beta(x, x) = 1$$

for every $x, y, z \in X, s, t \in S$. The set

$$Z^2(X, S(S)) = \{\beta : X \times X \rightarrow \text{Sym}(S), \text{ such that satysfies (C) and (Q)}\}$$

is the set of the non-abelian 2-cocycles with coefficients in $\text{Sym}(S)$.

Example 2.2. *Let X be a quandle. The map*

$$1 : X \times X \rightarrow \text{Sym}(S), \quad (x, y) \rightarrow 1$$

is a cocycle, then $Z^2(X, S)$ is non empty.

Remark 2.3. *The cocycle condition implies that*

$$(WCC) \quad \beta(xy, xz) = \beta(x, yz) \iff \beta(x, z) = \beta(y, z)$$

for every $x, y, z \in X$. We will call this condition weaker cocycle condition and we will denote it by WCC.

Cocycles with coefficients in groups different from permutations group still make sense and they have applications to other problems (see [1]).

Proposition 2.4. [1, Definition 2.9] *Let X be a quandle, S be a non-empty set and $(X \times S, \cdot)$ a quandle. Then the map*

$$\pi : (X \times S, \cdot) \longrightarrow X, \quad (x, s) \mapsto x$$

is a covering if and only if

$$(x, s) \cdot (y, t) = (xy, \beta(x, y)(t))$$

for every $x, y \in X$, $s, t \in S$ for some $\beta \in Z(X, S)$.

Proof. The pair $((X \times S, \cdot), \pi)$ a covering if and only if

$$(1) \quad \pi((x, s) \cdot (y, t)) = \pi(x, s)\pi(y, t) = xy$$

$$(2) \quad (x, s) \cdot (y, t) = (x, r) \cdot (y, t)$$

for every $x, y \in X$ and $r, s, t \in S$. Condition (1) is satisfied if and only if

$$(x, s) \cdot (y, t) = (xy, \beta(x, y, s)(t))$$

for some $\beta : X \times X \times S \longrightarrow \text{Sym}(S)$, since every left-multiplication is a bijection. Condition (2) is equivalent to have

$$(x, s) \cdot (y, t) = (xy, \beta(x, y)(t))$$

Condition C is equivalent to left-distributivity for \cdot and Q is equivalent to idempotency. \square

We will denote the covering defined in Proposition 2.4 $(X \times_\beta S, \pi)$. Coverings of X can be view as pairs (Y, f) such that L factors through f .

Example 2.5. *Let X be a quandle and S be a non-empty set. Then $X \times_I S \simeq X \times (S, *)$ where $(S, *)$ is the projection quandle over S .*

Proposition 2.6. *Let X, Y be racks and let $f : Y \longrightarrow X$ be a projection, then the following are equivalent:*

- (1) (Y, f) is a covering of X ;
- (2) $Y \simeq_\beta X \times S$, for some $S \neq \emptyset$ and some cocycle β ;
- (3) there exists a rack morphism σ such that the following diagram is commutative

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ & \searrow L & \downarrow \sigma \\ & & L(Y) \end{array}$$

Proof. (1) \Leftrightarrow (2) It follows from [1, Proposition 2.11], where β is defined by setting $\beta(x, y) = h_{[xy]} L_{h_{[y]}^{-1}(s)} h_{[x]}^{-1}$ where $h_{[x]}$ is any bijection between S and $[x] = f^{-1}(\{x\})$, and the isomorphism is given by

$$\phi_Y : Y \longrightarrow X \times_\beta S, \quad x \mapsto (f(x), h_{[x]}(x))$$

(1) \Leftrightarrow (3) It follows by the isomorphism theorem for congruences. \square

3. NON ABELIAN COHOMOLOGY

Let us introduce the definition of isomorphic coverings.

Definition 3.1. [3, Definition 4.1] *Let X be a quandle and (Y, f) , (Z, g) be coverings of X . They are isomorphic if there exists an isomorphism ϕ such that the following diagram is commutative*

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ \downarrow \phi & \nearrow g & \\ Z & & \end{array}$$

According to this definition $(X \times_{\beta} S, \pi)$ and $(X \times_{\beta'} S, \pi)$ are isomorphic if and only if the following relation between the cocycles holds ([1, Definition 2.9]).

Definition 3.2. *We say that β and β' are cohomologous if there exists*

$$\gamma : X \rightarrow \text{Sym}(S)$$

such that

$$\beta'(x, y) = \gamma(xy) \beta(x, y) \gamma(y)^{-1}$$

for every $x, y \in X$. Then define the set

$$H^2(X, S) = Z^2(X, S) / \sim$$

is the second constant cohomology set of X with coefficient in $\text{Sym}(S)$.

Proposition 3.3. *Let X be a quandle, $(Y, f) \simeq X \times_{\beta} S$ and $(Z, g) \simeq X \times_{\beta'} S$ coverings. Then the following are equivalent:*

- (1) $(Y, f) \simeq (Z, g)$;
- (2) $(X \times_{\beta} S, \pi) \simeq (X \times_{\beta'} S, \pi)$;
- (3) $\beta \sim \beta'$.

Proof. The equivalence between (1) and (2) can be readed by the following diagram

$$\begin{array}{ccccc} Y & \xrightarrow{\phi} & Z & & \\ \downarrow \phi_Y & \searrow f & \nearrow g & \downarrow \phi_Z & \\ X \times_{\beta} S & \xrightarrow{\pi} & X & \xleftarrow{\pi} & X \times_{\beta'} S \end{array}$$

where ϕ_Y and ϕ_Z are defined as in 2.6.

(2) \Leftrightarrow (3) It follows since every isomorphism which satisfy $\pi \circ \phi = \pi$ is given by

$$\phi : X \times_{\beta} S \longrightarrow X \times_{\beta'} S, \quad (x, s) \mapsto (x, \gamma(x)(s))$$

where $\gamma(x) \in \text{Sym}(S)$ for every $x \in X$. □

Some examples of coverings can be found in the class of homogeneous quandles.

Proposition 3.4. *Let $X_1 = \mathcal{Q}(G, H_1, \alpha)$ and $X_2 = \mathcal{Q}(G, H_2, \alpha)$ be a homogeneous quandle, $H_1 \leq H_2$ and the map*

$$\pi : X_1 \longrightarrow X_2, \quad xH_1 \mapsto xH_2$$

Then (X_1, π) is a covering of X_2 .

Proof. The map π is surjective and the blocks of $\ker(\pi)$ have the cardinality of H_2/H_1 . Let $x, y \in G$, then

$$\begin{aligned}\pi(xH_1 \cdot yH_1) &= \pi(x\alpha(x^{-1}y)H_1) = x\alpha(x^{-1}y)H_2 = \\ &= xH_2 \cdot yH_2 = \pi(xH_1) \cdot \pi(yH_1)\end{aligned}$$

so π is a projection. We have that $\pi(xH_1) = \pi(yH_1)$ if and only if $x = yh$ for some $h \in H_2$. Then

$$\begin{aligned}xH_1 \cdot zH_1 &= yhH_1 \cdot zH_1 = yh\alpha(h^{-1}y^{-1}z)H_1 = \\ &= yhh^{-1}\alpha(y^{-1}z)H_1 = y\alpha(y^{-1}z)H_1 = \\ &= yH_1 \cdot zH_1\end{aligned}$$

for every $z \in G$, therefore (X_1, π) is a covering. \square

Note that Y and Z can be isomorphic as quandles but (Y, f) and (Z, g) may not be isomorphic as coverings of X .

4. NORMALIZED COCYCLES FOR LATIN QUANDLE

For latin quandles it is possible to define a special representative of the classes of $H^2(X, S)$ with some nice properties.

Definition 4.1. Let X be a latin quandle, $u \in X$ and $\beta \in Z^2(X, S)$. If

$$(N) \quad \beta(x, u) = 1$$

for every $x \in X$, then β is said to be u -normalized. This condition will be called the normalization condition.

Every class in $H^2(X, S)$ has a normalized representative.

Proposition 4.2. Let X be a latin quandle, $u \in X$ and $\beta \in Z^2(X, S)$. Then there exists a u -normalized cocycle β_u , such that $\beta_u \sim \beta$.

Proof. We want to find a suitable γ to get a u -normalized cocycle. Hence

$$\beta_u(x, u) = \gamma(xu)\beta(x, u)\gamma(u)^{-1} = 1 \iff \gamma(xu) = \gamma(u)\beta(x, u)^{-1}$$

for every $x \in X$. Hence we get that

$$\gamma(x) = \gamma(u)\beta(x/u, u)^{-1}$$

The map γ is well defined since

$$\gamma(u) = \gamma(u)\beta(u/u, u)^{-1} = \gamma(u)\beta(u, u)^{-1} = \gamma(u)$$

So γ is unique up to the choice of $\gamma(u)$, so we can choose $\gamma(u) = 1$. \square

Notation 4.3. Let $\beta \in Z^2(X, S)$ and $u \in X$. We will denote by β_u the u -normalized cocycle cohomologous to β .

Proposition 4.4. Let X be a latin quandle, $u \in X$ and $\beta, \beta' \in Z^2(X, S)$. Then $\beta \sim \beta'$ if and only if

$$\beta'_u(x, y) = a\beta_u(x, y)a^{-1}$$

for some $a \in S$. Then $\beta \sim \mathbf{1}$ if and only if $\beta_u = \mathbf{1}$, for every $u \in X$.

Proof. Clearly $\beta \sim \beta'$ if and only if $\beta_u \sim \beta'_u$. Then there exists $\gamma : X \longrightarrow \text{Sym}(S)$ such that

$$\beta'_u(x, y) = \gamma(xy) \beta(x, y) \gamma(y)^{-1}$$

for every $x, y \in X$. Since $\beta_u(x, u) = \beta'_u(x, u) = 1$ for every $x \in X$, we have

$$\gamma(xu) = \gamma(u)$$

for every $x \in X$. Since R_u is a permutation we get that γ is a constant map. The second statement follow since $\mathbf{1}$ is a u -normalized cocycle. \square

So in order to prove that $H^2(X, S) = \{\mathbf{1}\}$ is equivalent to show that $\beta_u = \mathbf{1}$ for every $\beta \in Z^2(X, S)$.

Proposition 4.5. *Let X be a latin quandle, $u \in X$ and $\beta_u \in Z^2(X, S)$ a u -normalized cocycle, then the following equivalent identities hold*

- (1) $\beta(u, x) = 1$ for every $x \in X$;
- (2) $\beta(ux, uy) = \beta(x, y)$ for every $x, y \in X$.

Proof. First we prove that (1) and (2) are equivalent and then we prove just (1).

(1) \Rightarrow (2) It follows from C, since

$$\beta(ux, uy) \stackrel{(1)}{=} \beta(ux, uy) \beta(u, y) \stackrel{C}{=} \beta(u, xy) \beta(x, y) \stackrel{(1)}{=} \beta(x, y)$$

(2) \Rightarrow (1) Let $x = u/y$, then

$$\begin{aligned} \beta(u, y) &\stackrel{C}{=} \beta(u(u/y), uy)^{-1} \beta(u, (u/y)y) \beta(u/y, y) = \\ &= \beta(u(u/y), uy)^{-1} \beta(u, u) \beta(u/y, y) \stackrel{Q}{=} \\ &= \beta(u(u/y), uy)^{-1} \beta(u/y, y) \stackrel{(2)}{=} 1 \end{aligned}$$

for every $y \in X$.

Statement (1) follows since

$$\beta_u(u, yu) \stackrel{N}{=} \beta_u(u, yu) \beta_u(y, u) \stackrel{C}{=} \beta_u(uy, u) \beta_u(u, u) \stackrel{Q}{=} \beta_u(uy, u) = 1$$

for every $y \in X$ and since R_u is a bijection. \square

Proposition 4.6. *Let X be a latin quandle and β_u be a u -normalized cocycle. Then*

$$(3) \quad \beta_u(xy, xu) = \beta_u(x, yu)$$

for every $x, y \in X$.

Proof. Since

$$\beta_u(x, u) = \beta_u(y, u)$$

for every $x, y \in X$, we get

$$\beta_u(xy, xu) \stackrel{WCC}{=} \beta_u(x, yu)$$

for every $x, y \in X$. \square

Proposition 4.7. *Let X be a latin quandle and let β_u a u -normalized cocycle. Then*

$$(4) \quad \beta_u(x, y) = \beta_u(y/(x \setminus u) \cdot x, y)$$

for every $x, y \in X$.

Proof. Let $x, y \in X$, then

$$\begin{aligned}\beta_u(u/y, y) &\stackrel{N}{=} \beta_u(u/y \cdot x, u/y \cdot y) \beta_u(u/y, y) \stackrel{C}{=} \beta_u(u/y, xy) \beta_u(x, y) \\ \beta_u(u/y, y) &\stackrel{N}{=} \beta_u(x, u/y \cdot y) \beta_u(u/y, y) \stackrel{C}{=} \beta_u(x \cdot u/y, xy) \beta_u(x, y)\end{aligned}$$

then

$$\beta_u(u/y, xy) = \beta_u(x \cdot u/y, xy)$$

for every $x, y \in X$. Setting $u/y = z$ and $xy = v$, we have $x = v/y = v/(z \setminus u)$. So

$$\beta_u(z, v) = \beta_u(v/(z \setminus u) \cdot z, v)$$

for every $z, v \in X$. □

Lemma 4.8. *Let X be a latin quandle, and let β be a u -normalized cocycle, then*

$$\beta(u/(u/x), x) = \beta(u/x, x)$$

for every $x \in X$.

Proof. Setting $x = u/y$ and $y = u/z$ in C we get

$$\beta(u/(u/z), z) = \beta(u/z, z)$$

for every $z \in X$. □

4.1. Actions preserving normalized cocycles. Some of the identities we showed in the previous section can be stated as the invariance of normalized cocycles under the action of a permutation group on $X \times X$. In this way the relations given by the cocycle condition can be partially recovered through this action. In this section we will define this action and describe some properties of its orbits.

Proposition 4.9. *Let X be a latin quandle and β_u a u -normalized cocycle. Then β_u is invariant under the diagonal action of $\langle L_u \rangle$.*

Proof. From Proposition 4.5 we have that β_u is invariant under the action of the generator of $\langle L_u \rangle$, hence it is invariant under the action of the whole group. □

Notation 4.10. *We will denote by $\widehat{L_u}$ the diagonal action of L_u and we will use the following notation*

$$\begin{aligned}O_u(x) &= \{L_u^k(x), k \in \mathbb{N}\}, \quad l(x) = |O_u(x)| \\ \Delta(x, y) &= \{(L_u^k(x), L_u^k(y)), k \in \mathbb{N}\}, \quad l(x, y) = |\Delta(x, y)| \\ \Delta &= \{\Delta(x, y), x, y \in X\}\end{aligned}$$

for every $x, y \in X$.

Proposition 4.11. *Let X a latin quandle then $l(x, y) = l.c.m.\{l(x), l(y)\}$ for every $(x, y) \in X \times X$.*

Proof. Let $x, y \in X$, then

$$(L_u^k(x), L_u^k(y)) = (x, y) \Leftrightarrow k \mid l(x) \text{ and } k \mid l(y)$$

Since $l(x, y)$ is the minimum integer which satisfy this property, we have

$$l((x, y)) = l.c.m.\{l(x), l(y)\}$$

□

Proposition 4.12. *Let X be a finite latin quandle, $u \in X$, the map*

$$f : X \times X \longrightarrow X \times X, \quad (x, y) \mapsto (x(y/u), xu)$$

is a permutation and β_u is invariant under the action of $\langle f \rangle$.

Proof. Let assume that

$$f(x, y) = (x(y/u), xu) = (z(w/u), zu) = f(z, w)$$

Then

$$\begin{cases} xu = zu \\ x(y/u) = z(w/u) \end{cases} \iff \begin{cases} x = z \\ y/u = w/u \end{cases} \iff \begin{cases} x = z \\ y = w \end{cases}$$

Therefore f is injective and then bijective.

From Proposition 4.6, we have that β_u is invariant under the action of the generator of $\langle f \rangle$, hence it is invariant under the action of the whole group. \square

Notation 4.13. *We will denote by $F(x, y)$ the orbit under f of (x, y) .*

Proposition 4.14. *Let X be a latin quandle and let $x, y \in X$. Then*

$$f^k(x, y) = (x_k, x_{k-1}u)$$

where

$$x_k = \begin{cases} x_{-1} = y/u \\ (L_x L_{y/u})^{\frac{k}{2}}(x), \text{ if } k \text{ is even} \\ (L_x L_{y/u})^{\frac{k+1}{2}}(y/u), \text{ if } k \text{ is odd} \end{cases}$$

for every $k \in \mathbb{Z}$.

Proof. Set $x_{-1} = y/u = z$ and set $f^k(x, y) = (x_k, y_k)$. By definition we have

$$(5) \quad x_0 = x = (L_x L_z)^0(x)$$

$$(6) \quad x_1 = xz = x(zz) = (L_x L_z)^1(z)$$

and then $f(x, y) = (x_0 x_{-1}, x_0 u)$. By induction it follows that

$$f^{k+1}(x, y) = f(x_k, x_{k-1}u) = (x_k x_{k-1}, x_k u)$$

Since 5 and 6 holds, then by induction we have

$$\begin{aligned} x_{2k+1} &= x_{2k} x_{2k-1} = \left((L_x L_z)^k(x) \right) \left((L_x L_z)^k(z) \right) = \left((L_x L_z)^k \right) (xz) \\ &= \left((L_x L_z)^k L_x \right) (z) = \left((L_x L_z)^k (L_x L_z) \right) (z) = \\ &= \left((L_x L_z)^{k+1} \right) (z) \end{aligned}$$

And

$$\begin{aligned} x_{2k+2} &= x_{2k+1} x_{2k} = \left(\left((L_x L_z)^{k+1} \right) (z) \right) (L_x L_z)^k(x) = \\ &= (L_x L_z)^k \left((L_x L_z) (z) x \right) = \left((L_x L_z)^k \right) (L_x(z) x) = \\ &= \left((L_x L_z)^k \right) (L_x L_z L_x^{-1}(x)) \\ &= \left((L_x L_z)^{k+1} \right) (x) \end{aligned}$$

\square

The map f preserves the product.

Proposition 4.15. *Let X be a latin quandle and the map*

$$p : X \times X \longrightarrow X, \quad (x, y) \mapsto xy$$

Then

$$p(x, y) = p(f(x, y))$$

for every $x, y \in X$.

Proof. We have that

$$p(f(x, y)) = p(x \cdot y/u, xu) = x(y/u) \cdot xu = x \cdot (y/u)u = xy = p(x, y)$$

for every $x, y \in X$. \square

By this property you can check the lenght of the orbits under f just on one of the two components.

Proposition 4.16. *Let X be a latin quandle and $x, y \in X$. Then the following are equivalent:*

- (1) $f^k(x, y) = (x, y)$;
- (2) $x_k = x$;
- (3) $x_{k-1} = y/u$.

Proof. Clearly (1) implies (2) and (3). Moreover (2) and (3) together imply (1). If (2) holds, since by Proposition 4.15, f preserves the product, then we have

$$p(f^k(x, y)) = x_k \cdot x_{k-1}u = x \cdot x_{k-1}u = xy$$

And since X is a quandle $y = x_{k-1}u$. The same argument shows that (3) \Rightarrow (2), then (2) and (3) are equivalent. Therefore both the implication (2) \Rightarrow (1) and (3) \Rightarrow (1) hold. \square

Corollary 4.17. *Let X be a latin quandle. Then $(x, y) \in \text{Fix}(f)$ if and only if $y = xu$.*

Proof. It follows from Proposition 4.16 (3). \square

Corollary 4.18. *Let X be a latin quandle and let $x, y \in X$. Then the following are equivalent:*

- (1) $F(x, y) \cap \{(z, u), z \in X\} \neq \emptyset$;
- (2) $F(x, y) \cap \{(u, z), z \in X\} \neq \emptyset$;
- (3) $F(x, y) \cap \{(z, z), z \in X\} \neq \emptyset$.

Proof. It follows since we have that

$$\begin{aligned} f(u, xu) &= (ux, uu) = (ux, u) \\ f^2(u, xu) &= (ux \cdot u, ux \cdot u) = (uxu, uxu) \end{aligned}$$

for every $x \in X$. \square

Proposition 4.19. *Let X be a finite latin quandle and $u \neq y \in X$. Then the map:*

$$\omega : X \times X \longrightarrow X \times X, \quad (x, y) \mapsto (y/(x \setminus u) \cdot x, y) = (\omega_y(x), y)$$

is a permutation for every $u \in X$. Moreover

$$(7) \quad \beta_u(x, y) = \beta_u(\omega(x, y))$$

Proof. Clearly ω is a permutation if and only if ω_y is a permutation for every $y \in X$. Let us denote

$$\begin{aligned} x \backslash u &= a, & z \backslash u &= b \\ u_x &= y / (x \backslash u), & u_z &= y / (z \backslash u) \end{aligned}$$

The map $x \mapsto u_x$ is bijective by [8, Proposition 2.3]. Let $x, z \in X$ such that $u_x x = \omega_u(x, y) = \omega_u(z, y) = u_z z$, then

$$\begin{aligned} u_x(xa) &= u_x u \\ u_x(xa) &= u_x x \cdot u_x a = u_x x \cdot y = \\ &= u_z z \cdot y = u_z z \cdot u_z b = \\ &= u_z \cdot zb = u_z u \end{aligned}$$

therefore $u_x = u_z$, which implies $x = z$. The map ω_y is so injective and then bijective for every $y \in X$. Formula 7 follows from 4.7. \square

Proposition 4.20. *Let X be a latin quandle, then $\omega(x, y) = (x, y)$ if and only if $y = u$.*

Proof. The statement is equivalent to have that ω_y has no fixed points whenever $y \neq u$ and that $\omega_u = id_X$. Let $x, y \in X$ such that

$$\omega(x, y) = (y / (x \backslash u) \cdot x, y) = (x, y)$$

if and only if $y / (x \backslash u) = x$, which holds only when $y = u$. \square

The map ω does not preserve the product.

Proposition 4.21. *Let X be a latin quandle. Then*

$$p(\omega(x), y) = p(x, y) = xy$$

if and only if $y = u$.

Proof. We have that

$$p(\omega(x, y), y) = (y / (x \backslash u) \cdot x)y = xy$$

is equivalent to have $y / (x \backslash u) = x$ and this is true if and only if $y = u$. \square

We have that the action of f and ω on $X \times X$ induces an action on Δ .

Proposition 4.22. *Let X be a latin quandle and $G = \langle f, \omega \rangle$. Then*

$$(8) \quad G \curvearrowright \Delta, \quad g(\Delta(x, y)) = \Delta(g(x, y))$$

defines a group action of G on Δ .

Proof. It is enough to show that f and ω commutes with \widehat{L}_u . Let $x, y \in X$, then

$$\begin{aligned} f\widehat{L}_u(x, y) &= f(ux, uy) = (ux \cdot (uy)/u, uxu) = \\ &= (ux \cdot u(y/u), uxu) = (u \cdot x(y/u), uxu) = \\ &= \widehat{L}_u(x(y/u), xu) = \widehat{L}_u f(x, y) \end{aligned}$$

Moreover

$$\begin{aligned}
\omega(\widehat{L}_u(x, y)) &= \omega(ux, uy) = \\
&= (L_{R_{L_{ux}(u)}^{-1}}(uy)(ux), uy) = (L_{L_u R_{L_{ux}(u)}^{-1}} L_u^{-1}(uy)(ux), uy) \\
&= (L_u L_{R_{L_{ux}(u)}^{-1}}(y) L_u^{-1}(ux), uy) = (L_u L_{R_{L_{ux}(u)}^{-1}}(y)(x), uy) = \\
&= (u\omega_{y,u}(x), uy) = \widehat{L}_u \omega(x, y)
\end{aligned}$$

Then the action defined as in 8 is well defined. \square

The maps f and ω do not commute.

Proposition 4.23. *Let X be a latin quandle, then*

$$(f\omega)(x, y) = (\omega f)(x, y)$$

if and only if $x = y = u$.

Proof. Let $x, y \in X$ and assume that $f\omega(x, y) = \omega f(x, y)$. Since

$$\begin{aligned}
f\omega(x, y) &= (\omega_y(x) \cdot y/u, \omega_y(x)u) \\
\omega f(x, y) &= (\omega_{xu}(x \cdot y/u) \cdot x(y/u), xu)
\end{aligned}$$

we have that $\omega_{y,u}(x) = x$, and then $y = u$ by Proposition 4.20. So it follows that $\omega_{xu,u}(xu) = xu$, hence by Proposition 4.20 we have that $xu = u$ and therefore $x = u$. \square

The only fixed point of $X \times X$ under the action of G is (u, u) . If the action is transitive on $X \times X \setminus \{(u, u)\}$, then $H^2(X, S) = \{1\}$. For the group G the following proposition holds.

Proposition 4.24. *Let X be a latin quandle and $G = \langle L_u, f, \omega \rangle$. If*

$$X = \bigcup_{x \in X} O_G(x, x)$$

then $H^2(X, S) = \{1\}$ for every S .

Proof. Let β be a u -normalized cocycle. We have that

$$\beta(x, u) = \beta(u, x) = \beta(x, x) = 1$$

By Corollary 4.18, if $X = \bigcup_{x \in X} O_G(x, x)$ then $\beta = 1$. \square

Let us see some properties of the orbits under the action of G .

Proposition 4.25. *Let X be a latin quandle. Then \widehat{L}_u decomposes $\text{Fix}(f)$ and $p^{-1}(\{u\})$.*

Proof. It follows since

$$\begin{aligned}
f\widehat{L}_u(z, zu) &= \widehat{L}_u f(z, zu) = \widehat{L}_u(x, x, u) \\
p\widehat{L}_u(x, y) &= ux \cdot uy = u \cdot xy = u \cdot u = u
\end{aligned}$$

for every $z \in X$ and whenever $xy = u$. \square

Notation 4.26. *Let us denoted by*

$$\begin{aligned}
\Delta^f &= \{\Delta(x, xu), u \neq x \in X\} = \text{Fix}(f) \setminus \{(u, u)\} \\
\Delta_u &= \{\Delta(x, x \setminus u), u \neq x \in X\} = p^{-1}(\{u\}) \setminus \{(u, u)\}
\end{aligned}$$

Proposition 4.27. *Let X be a latin quandle then*

- (1) $\omega(\Delta(x, x \setminus u)) \notin \Delta_u$;
- (2) $\omega(\Delta(x, xu)) \notin \Delta^f$;

for every $x \in X$.

Proof. (1) It follows by Proposition 4.21.

(2) It follows by Proposition 4.23. □

5. NORMALIZED COCYCLES FOR CONNECTED AFFINE QUANDLES

This section is about cohomology of affine quandles. An affine representation allows us to exploit the group structure to understand better the behaviour of the orbits under the action of G .

We start with some remarks about the map α . Since in the class of finite Affine quandles latinity is equivalent to connectedness, all the previous results holds for finite connected affine quandles. Most of the following results holds in a more general setting.

Proposition 5.1. *Let $X = \mathcal{Q}(A, \alpha)$ be a finite affine quandle. Then the following are equivalent*

- (1) X is latin;
- (2) X is connected;
- (3) $1 - \alpha \in \text{Aut}(A)$.

Proof. It follows since $R_0 = (1 - \alpha)$ and since $O_{\text{LMit}(X)}(x) = x + \text{Im}(1 - \alpha)$. □

Proposition 5.2. *Let A be an Abelian group, $\alpha, 1 - \alpha \in \text{Aut}(A)$ and $x \in A$. Then*

$$(9) \quad \alpha^n(x) = x \iff \sum_{k=0}^{n-1} \alpha^k(x) = 0$$

Proof. It follows since

$$(1 - \alpha) \sum_{k=0}^{n-1} \alpha^k(x) = (1 - \alpha^n)(x) = 0 \iff \sum_{k=0}^{n-1} \alpha^k(x) = 0 \iff \alpha^n(x) = x$$

□

Proposition 5.3. *Let $X = \mathcal{Q}(A, \alpha)$ be an affine quandle, then*

$$x_0 \cdot (x_1 \cdot (x_2 \cdot (\dots (x_{n-1} \cdot x_n) \dots))) = x_0 + \sum_{k=1}^n (-1)^k \alpha^k(x_k - x_{k-1})$$

for every $x_0, \dots, x_n \in X$.

Proof. Let us consider

$$x_0 \cdot x_1 = x_0 + \alpha(x_1 - x_0)$$

Then by induction

$$\begin{aligned}
x_0 \cdot (x_1 \cdot (\dots \cdot (x_n \cdot x_{n+1}))) &= x_0 \cdot \left(x_1 + \sum_{k=2}^{n+1} \alpha^{k-1} (x_k - x_{k-1}) \right) = \\
&= x_0 + \alpha(x_1 - x_0) + \sum_{k=2}^{n+1} \alpha^k (x_k - x_{k-1}) = \\
&= x_0 + \sum_{k=1}^{n+1} \alpha^k (x_k - x_{k-1})
\end{aligned}$$

□

Proposition 5.4. *Let $X = \mathcal{Q}(A, \alpha)$ be a finite connected affine quandle and let $x, z = (1 - \alpha)^{-1}(y) \in X$. Then $|F(x, y)| = n$ if and only if it is the minimum natural such that*

$$\sum_{j=1}^n (-1)^j \alpha^j (x - z) = 0$$

holds.

Proof. It follows from Proposition 5.3 in view of Propositions 4.14 and 4.16. □

Corollary 5.5. *Let $X = \mathcal{Q}(A, \alpha)$ be a finite connected affine quandle and let $x, z = (1 - \alpha)^{-1}(y) \in X$ such that $|F(x, y)| = n$. Then*

$$(-1)^n \alpha^n (x - z) = x - z$$

Moreover if n is even, then $l(x - z)$ divides n . If n is odd then $l(x - z)$ divides $2n$.

Proof. Let $x, z = (1 - \alpha)^{-1}(y) \in X$ and $n = |F(x, y)|$. Then by Proposition 5.4 you have

$$\begin{cases} x_n = x + \sum_{k=1}^n (-1)^k \alpha^k (x - z) = x \\ x_{n-1} = x + \sum_{k=1}^{n-1} (-1)^k \alpha^k (x - z) = z \end{cases}$$

These equations together imply that $(-1)^n \alpha^n (x - z) = x - z$.

So if n is even then $l(x - z)$ divides n . Otherwise we have

$$\alpha^{2n} (x - z) = -\alpha^n (x - z) = x - z$$

Therefore $l(x - z)$ divides $2n$. □

Lemma 5.6. *Let $X = \mathcal{Q}(G, \alpha)$ a connected affine quandle and β a 0-normalized cocycle. Then*

$$(10) \quad \omega_y(x) = y + x$$

$$(11) \quad \beta(ny + x, y) = \beta(x, y)$$

$$(12) \quad \beta(nx, x) = 1$$

for every $n \in \mathbb{N}$ and every $x, y \in X$.

Proof. Let $x, y \in X$ and $z = x \setminus 0 = x - \alpha^{-1}(x)$, then

$$\begin{aligned}
\omega_{y,0}(x) &= y / (x \setminus 0) \cdot x = y / z \cdot x \\
&= (z + (1 - \alpha)^{-1}(y - z)) \cdot x = (1 - \alpha)(z) + y - z + \alpha(x) = \\
&= y + x
\end{aligned}$$

Formula 11 follows from 7. Formula 12 follows from Q and 11. □

In the affine case is possible to compute the lenght of the orbits of f from the lenght of the orbits of α and by the order of the elements of the group.

Lemma 5.7. *Let $X = \mathcal{Q}(A, \alpha)$ be a finite connected affine quandle and let $x, z = (1 - \alpha)^{-1}(y) \in A$. Assume that $l(x - z)$ is odd, then*

$$|F(x, y)| = \begin{cases} l(x - z), & \text{if } o(x - z) = 2 \\ 2l(x - z), & \text{otherwise} \end{cases}$$

Proof. Let $l = l(x - z)$ and $F = |F(x, y)|$.

If F is even, then by Corollary 5.5 $F = rl$ for some even r . Therefore, by Proposition 5.4, r is the minimum even natural for which

$$(13) \quad \sum_{j=1}^{rl} (-1)^{-1} \alpha^j(x - z) = 0$$

holds. Since l is odd then $r = 2$ satisfies 13, then $r = 2$ and so $F = 2l$.

If F is odd, then by Corollary 5.5 l divides $2F$ and since it is odd then l divides F . Moreover by Corollary 5.5 $o(x - z) = 2$. Therefore by Proposition 5.4, r is the minimum natural for which

$$(14) \quad \sum_{j=1}^{rl} (-1)^{-1} \alpha^j(x - z) = \sum_{j=1}^{rl} \alpha^j(x - z) = 0$$

holds. Since $r = 1$ satisfies 14, then $r = 1$ and so $F = l$.

If $F = l$ then by Corollary 5.5 we have

$$(-1)^l \alpha^l(x - z) = -(x - z) = x - z$$

and then $o(x - z) = 2$, and this completes the proof. \square

Lemma 5.8. *Let $X = \mathcal{Q}(A, \alpha)$ be a finite connected affine quandle and let $x, z = (1 - \alpha)^{-1}(y) \in A$. Assume that $l = l(x - z)$ is even, then*

$$|F(x, y)| = \begin{cases} kl, & \text{if } |F(x, y)| \text{ is even} \\ k' \frac{l}{2}, & \text{otherwise} \end{cases}$$

where $k = o\left(\sum_{k=1}^l (-1)^k \alpha^k(x - z)\right)$, $k' = o\left(\sum_{k=1}^{\frac{l}{2}} (-1)^k \alpha^k(x - z)\right)$.

Proof. Let $l = l(x - z)$, $F = |F(x, y)|$.

If F is even the by Corollary 5.5 $F = rl$ for some r . Since l is even we have that

$$(15) \quad \sum_{k=1}^{rl} (-1)^k \alpha^k(x - z) = r \sum_{k=1}^l (-1)^k \alpha^k(x - z) = 0$$

and r is the minimum for which equation 15 holds. Then by definition

$$r = o\left(\sum_{k=1}^l (-1)^k \alpha^k(x - z)\right)$$

Let F be odd, then by Corollary 5.5 $F = (2s + 1) \frac{l}{2}$ for some s , and by Corollary 5.5 we have that $\alpha^{\frac{l}{2}}(x - z) = -(x - z)$. Hence we get that

$$(16) \quad \sum_{k=1}^{(2s+1)\frac{l}{2}} (-1)^k \alpha^k(x - z) = (2s + 1) \sum_{k=1}^{\frac{l}{2}} (-1)^k \alpha^k(x - z) = 0$$

and s is the minimum for which equation 16 holds. By definition

$$2s + 1 = o \left(\sum_{k=1}^{\frac{l}{2}} (-1)^k \alpha^k (x - z) \right)$$

□

Lemma 5.9. *Let $X = \mathcal{Q}(A, \alpha)$ be a connected affine quandle, then the following are equivalent:*

- (1) $|O_u(x)| \neq 2$ for every $x \in X$;
- (2) the map:

$$\begin{aligned} g : X &\longrightarrow X \\ x &\mapsto x \cdot (x \cdot 0) \end{aligned}$$

is bijective;

Proof. The statement are equivalent since

$$g(x) = x \cdot (x \cdot 0) = (1 - \alpha^2)(x)$$

for every $x \in X$ and then $g = (1 - \alpha^2)$.

□

Lemma 5.10. *Let $X = \mathcal{Q}(G, \alpha)$ be a latin affine quandle, then*

- (1) $(\omega(0/x, x)) \in \text{Fix}(f)$ if and only if $o(x) = 2$;
- (2) $(0/(0/x), x) \in \text{Fix}(f)$ if and only if $(\alpha^2 + \alpha - 1)(x) = 0$.

Proof. (1) We have that

$$(0/x + x) \cdot 0 = (1 - \alpha) \left(2x - (1 - \alpha)^{-1}(x) \right) = x$$

holds if and only if $2x = 0$.

(2) We have that

$$(0/(0/x)) \cdot 0 = (1 - \alpha) \left(x - 2(1 - \alpha)^{-1}(x) + (1 - \alpha)^{-2}(x) \right) = x$$

holds if and only if $(\alpha^2 + \alpha - 1)(x) = 0$.

□

Let $X = \mathcal{Q}(A, \alpha)$ be a finite connected affine quandle. If $|F(x, y)| = |X| - 1$ for every $x, y \in X$, then $|O_0(x)| \neq 2$ for every $x \in X$. This follows since f decomposes $p^{-1}(c)$ in two orbits respectively of size $|X| - 1$ and 1. This is equivalent to (3) of Lemma 5.9. Under this assumptions we have that $|\Delta_u| = |\Delta^f| = 1$ and $\beta(x, y) = 1$ for every $(x, y) \notin \Delta_u \cup \Delta^f$, so we have to show that $\beta|_{\Delta_u \cup \Delta^f} = \mathbf{1}$. By Proposition 4.27 it is enough to show that $\beta|_{\Delta_u} = \mathbf{1}$.

Proposition 5.11. *Let $X = \mathcal{Q}(A, \alpha)$ be a finite connected affine quandle. If $\exp(A) \neq 2$ and $|F(x, y)| = |X| - 1$ for every $x, y \in X$, then $H^2(X, S) = \{\mathbf{1}\}$.*

Proof. By Lemma 5.10 (1) it follows that there exists $x \in A$ such that $\omega(x, x \setminus u) \notin \Delta_u \cup \Delta^f$. Therefore $\beta|_{\Delta_u} = \mathbf{1}$. □

Proposition 5.12. *Let $X = \mathcal{Q}(A, \alpha)$ be a connected affine quandle. If $\exp(A) = 2$, $o(\alpha) \neq 3$ and $|F(x, y)| = |X| - 1$ for every $x, y \in X$, then $H^2(X, S) = \{\mathbf{1}\}$.*

Proof. By Lemma 5.10 (2), if $o(\alpha) \neq 3$ we have that there exists $x \in X$ such that

$$(\alpha^2 + \alpha - 1)(x) \stackrel{\exp(A)=2}{=} (\alpha^2 + \alpha + 1)(x) \neq 0$$

and then by Proposition 4.8, $\beta|_{\Delta_u} = \mathbf{1}$. \square

Proposition 5.13. ([6, Lemma 3]) *Let X be a rack of prime size p . Then $X \simeq \mathcal{Q}(\mathbb{Z}_p, q)$ for some $q \in \text{Aut}(\mathbb{Z}_p)$.*

Let us see how this well-known result about cohomology of quandles of prime order follows from this general construction.

Proposition 5.14. [2, Lemma 5.1] $H^2(\mathcal{Q}(\mathbb{Z}_p, q), S) = \{\mathbf{1}\}$ for every S .

Proof. It follows from formula 12, since every element generates the group. \square

Corollary 5.15. *Let p_1, p_2 be prime integers. Every connected quandle of order $p_1 p_2$ is faithful.*

Proof. Let X be a quandle of order $p_1 p_2$. If X is not faithful, then $L(X)$ has order p_i and

$$X \simeq L(X) \times_{\beta} S \simeq \mathcal{Q}(\mathbb{Z}_{p_i}, q_i) \times_{\mathbf{1}} S$$

for $i = 1, 2$, and then X is not connected. \square

6. CONNECTED QUANDLES OVER CYCLIC GROUPS.

Now we apply these results to the family of connected affine quandles over cyclic groups, in order to extend the result given by Lemma [2, Lemma 5.1].

Proposition 6.1. *Let $X = \mathcal{Q}(\mathbb{Z}_m, \lambda_n)$ be a quandle, where*

$$\lambda_n : \mathbb{Z}_m \rightarrow \mathbb{Z}_m, \quad k \mapsto nk$$

Then X is a connected quandle if and only if $G.C.D.\{1 - n, m\} = G.C.D.\{n, m\} = 1$. Moreover m is odd.

Proof. The map λ_n is an automorphism if and only if $G.C.D.\{n, m\} = 1$. By Proposition 5.1 X is connected if and only if $1 - \lambda_n$ is an automorphism. This is equivalent to have $M.C.D.\{1 - n, m\} = 1$.

Then m has to be odd, otherwise one of this two condition fails. \square

For this quandles we have a bigger group which preserves normalized cocycles.

Proposition 6.2. *Let $X = \mathcal{Q}(\mathbb{Z}_m, \lambda_n)$ be a connected quandle and β be a 0-normalized cocycle. Then*

- (1) $\beta(k, u) = 1$, for every $u \in U(\mathbb{Z}_m)$ and $k \in \mathbb{Z}_m$;
- (2) $\beta(u, k) = 1$, for every $u \in U(\mathbb{Z}_m)$ and $k \in \mathbb{Z}_m$;
- (3) β is invariant under the diagonal action of $U = \langle L_u, u \in U(\mathbb{Z}_m) \rangle$.

Proof. In view of Proposition 4.5 we have that (2) and (3) are equivalent, and by Proposition 4.5, (1) implies (2). So we need to prove just (1). Since every invertible elements generated the group, by formula 12 then we have

$$\beta(k, u) = 1.$$

for every $u \in U(\mathbb{Z}_m)$ and every $k \in \mathbb{Z}_m$. \square

Proposition 6.3. *Let m be a odd natural number. Then every element $x \notin U(\mathbb{Z}_m)$ can be written as*

$$x = u + v$$

for some $u, v \in U(\mathbb{Z}_m)$.

Proof. Let $m = \prod_{k=1}^r p_k^{\alpha_k}$. By the canonical decomposition of we have that every element $x \in \mathbb{Z}_m$ is given by

$$x = x_1 + \dots + x_r$$

with $x_i \in \mathbb{Z}_{p_i^{\alpha_i}}$. By the chinese remainder theorem we have that

$$U(\mathbb{Z}_m) \simeq \prod_{k=1}^r U(\mathbb{Z}_{p_k^{\alpha_k}})$$

Let $x = x_j$, then it is a nilpotent element and then $u - x \in U(\mathbb{Z}_{p_j^{\alpha_j}})$ and then x is the sum of two invertible elements of $\mathbb{Z}_{p_j^{\alpha_j}}$. If $x_i \notin U(\mathbb{Z}_{p_i^{\alpha_i}})$ for every $1 \leq i \leq r$, then there exist $u_i, v_i \in U(\mathbb{Z}_{p_i^{\alpha_i}})$ such that $x_i = u_i + v_i$.

If $x_i \in U(\mathbb{Z}_{p_i^{\alpha_i}})$, since $p_i^{\alpha_i}$ is odd we have that $2 \in U(\mathbb{Z}_{p_i^{\alpha_i}})$, hence $x_i = 2x_i - x_i = u_i + v_i$, with $u_i, v_i \in U(\mathbb{Z}_{p_i^{\alpha_i}})$.

In any case, we can write

$$x_i = u_i + v_i$$

with $u_i, v_i \in U(\mathbb{Z}_{p_i^{\alpha_i}})$. Setting $u = u_1 + \dots + u_r$, $v = v_1 + \dots + v_r$, we have that $x = u + v$. \square

Theorem 6.4. *Let $X = \mathcal{Q}(\mathbb{Z}_m, \lambda_n)$ be a connected quandle then $H^2(X, S) = \{1\}$.*

Proof. Let $x \notin U(\mathbb{Z}_m)$. By Proposition 6.3, we have that $x = u + v$ for some invertible elements u, v . Then

$$x = (1 - n)^{-1}(1 - n)u + nn^{-1}v = (1 - n)^{-1}u \cdot n^{-1}v = u' \cdot v'$$

So U maps every element of X to some invertible element, therefore by Proposition 6.2 it follows that

$$\beta_0(x, y) = \beta_0(u' \cdot v', u' \cdot y') = \beta_0(v', y') = 1$$

for every $x, y \in X$. \square

7. MINIMAL QUANDLES

In this section we will talk about minimal quandles.

Definition 7.1. *A quandle is called minimal if every subquandle is trivial.*

Minimal quandles can be characterized by the following Proposition.

Proposition 7.2. *Let X be a quandle. Then it is minimal if and only if it is generated by every couple of elements $x, y \in X$.*

Proof. The statement is equivalent to say that every non trivial subquandle is the whole X . \square

Corollary 7.3. *Let X be a minimal quandle. Then every group of automorphisms is Frobenius.*

Proof. Let G be a group of automorphisms and $g \in G$ such that $g(x) = x$ and $g(y) = y$ for some $x, y \in X$. By 7.2 then $g = id_X$. \square

Proposition 7.4. *Let X be a finite minimal quandle and $|X| \neq 2$. Then $X \simeq \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ and α has no proper invariant subgroups.*

Proof. The projection quandle of size 2 is minimal but $Trans(X) = \{1\}$. By Corollary 7.3 $Trans(X)$ is a Frobenius group and then it has a regular nilpotent subgroup N ([11]). Then by [10, Theorem 4.1], $Trans(X)$ embeds in some quotients of N , so $Trans(X) = N$. By Lemma [4, Lemma 4.2] any proper normal subgroup invariant under α provides a proper quotient, and every proper quotient provides a proper subquandles since any block of a congruence is a subquandle. Then $Trans(X)$ has no proper normal subgroups invariant under α , in particular $Trans(X)$ has no proper characteristic subgroups. So $Trans(X)' = \{1\}$ and $Trans(X)$ is a p -group since every normal p -Sylow is characteristic. Finally since $\Phi(Trans(X)) = \{1\}$, then $Trans(X)$ is elementary Abelian. \square

Corollary 7.5. *Let X be a finite minimal quandle and $|X| \neq 2$. Then it is latin.*

Proof. It follows by Proposition 7.4, since they are affine and connected. \square

Proposition 7.6. *Let X be a finite minimal quandle. Then $Aut(X)$ is two-transitive.*

Proof. A group G acting on X is two-transitive if and only if $Stab_G(x)$ acts transitively on $X \setminus \{x\}$.

By Proposition 7.4 then $X \simeq \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$. Let $x \in X$, consider the following equation

$$\sum_{i=0}^n a_i \alpha^i(x) = 0$$

if it holds for some non-zero choice of coefficients, then the subgroups generated by the set $B_x = \{\alpha^i(x), 0 \leq i \leq n-1\}$ would be invariant under α . Then the set B_x is a base for \mathbb{Z}_p^n . Then the map

$$f_{\mathbf{a}} : X \longrightarrow X, \quad x \mapsto \sum_{i=0}^n a_i \alpha^i(x)$$

is an automorphism for every non-zero choice of $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}_p^n$, since B_x is a base for every $x \in X$. Then

$$\mathcal{F} = \langle f_{\mathbf{a}}, \mathbf{a} \in \mathbb{Z}_p^n \rangle$$

is a regular subgroup of $Stab(0)$ in $Aut(X)$, since it is Abelian. The size of \mathcal{F} is $p^n - 1$, then it is transitive on $X \setminus \{0\}$, therefore $Aut(X)$ is two-transitive. \square

Proposition 7.7. *Let X be a quandle such that $Aut(X)$ acts two-transitively on X . Let $t(x, y), s(x, y)$ be binary terms. If the identity*

$$t(x, y) = s(x, y)$$

holds for some pair $(x, y) \in X \times X$, then it holds for every pair $(z, t) \in X \times X$.

Proof. Assume that

$$t(x, y) = s(x, y)$$

hold for some $x, y \in X$. Hence since

$$h(t(x, y)) = t(h(x), h(y)) = h(s(x, y)) = s(h(x), h(y))$$

for every $h \in \text{Aut}(X)$, then it holds for every pair $(z, t) \in X \times X$, since $\text{Aut}(X)$ is two-transitive. \square

Minimal quandles are affine over an elementary Abelian group and by the two-transitivity of the action of $\text{Aut}(X)$ then we have the following.

Corollary 7.8. *Let X be a finite minimal quandle. Then the non trivial orbits of α has all the same lenght.*

Proof. It follows by Proposition 7.7, since the lenght of the α orbits is determined by an equation between binary terms. \square

Corollary 7.9. *Let $X = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be a minimal quandle. Then all non trivial f -orbit have the same lenght and all the non trivial ω -orbits have size p .*

Proof. By Proposition 4.14 we have that the lenght of the orbits under the action of $\langle f \rangle$ is determined by an equation between binary terms (see Proposition 4.14). Hence by Proposition 7.7 we have that the non trivial orbits have all the same lenght. The second statement follows by Lemma 5.6. \square

Notation 7.10. *We will denote by F the size of all the non-trivial f -orbits.*

Corollary 7.11. *Let $X = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be minimal quandle for some $n > 1$. Then F divides $|X| - 1$.*

Proof. By Corollary 7.8 X the orbits of α have all the same size. By [7, Corollary 7.3] every involutory affine quandle is isomorphic to $X \simeq \mathcal{Q}(A, -id_A)$, which is not minimal, since every subgroup is invariant under α .

Then by Lemma 5.9 every set $p^{-1}(c) = \{(x, y) \in X \times X, xy = c\}$ contains just one f -fixed point.

The map f decomposes these sets in orbits of the same size F , then F divides $|X| - 1$. \square

Lemma 7.12. *Let $X = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be minimal quandle for some $n > 1$. Then if $o(\alpha)$ is odd*

$$F = \begin{cases} o(\alpha), & \text{if } p = 2 \\ 2o(\alpha), & \text{otherwise} \end{cases}$$

If $o(\alpha)$ is even then

$$F = \begin{cases} o(\alpha), & F \text{ is even} \\ \frac{o(\alpha)}{2}, & \text{otherwise} \end{cases}$$

Proof. The first statement follows by Lemma 5.7, since $l(x) = o(\alpha)$ for every $x \in X$. Since F divides $|X| - 1$ by Lemma 5.8, necessarily $F = o(\alpha)$ when it is even and $F = \frac{o(\alpha)}{2}$ otherwise. \square

We have the following characterization for two-transitive quandles.

Theorem 7.13. ([9, Corollary 4]) *Let X be a quandle. Then $LMlt(X)$ is two-transitive if and only if*

$$X \simeq \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$$

for some prime integer p , some natural n and $\alpha \in GL_n(p)$ with $o(\alpha) = |X| - 1$.

So in particular two-transitive quandles are minimal.

Lemma 7.14. *Let X be a latin quandle such that $l(x) = o(\alpha)$ for every $x \in X$. Then*

$$F(x, y) = |O_{\langle f \rangle}(\Delta(x, y))|$$

for every $x, y \in X$ such that $xy \neq u$.

Proof. Under this assumption by Proposition 4.11, $|\Delta(x, y)| = o(\alpha)$. Assume that $f^k(\Delta(x, y)) = \Delta(x, y)$, then

$$f(x, y) = \widehat{L_u}^r(x, y)$$

which implies $p(x, y) = xy = L_u^r(xy) = p(\widehat{L_u}^r(x, y))$. Then r divides $o(\alpha) = |\Delta(x, y)|$, therefore $f(x, y) = (x, y)$. \square

By Lemma 7.14 we have that for minimal quandles F coincides with the length of the orbits of the action of f on Δ .

Proposition 7.15. *Let $X = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be a two-transitive quandle, then*

- (1) *if $p = 2$ then $F = |X| - 1$;*
- (2) *$F = |X| - 1$ if it is even and $F = \frac{|X|-1}{2}$ if it is odd, otherwise.*

Moreover Δ_0 and Δ^f are one element sets.

Proof. Two-transitive quandles are minimal. By Lemma 7.12, if $p = 2$ then $|X| - 1$ is odd, hence $F = |X| - 1$.

The second statement follows by 7.12 since $|X| - 1$ is even.

The last statement follows since every diagonal has size $|X| - 1$. \square

Proposition 7.16. *Let $X = \mathcal{Q}(\mathbb{Z}_p^n, \alpha)$ be a two-transitive quandle with $p \geq 3$ and $n > 1$. Then $H^2(X, S) = \{1\}$.*

Proof. If $F = |X| - 1$, it follows from Proposition 5.11.

Let us assume $F = \frac{|X|-1}{2}$, then the map f decomposes $\Delta \setminus (\Delta_u \cup \Delta^f)$ in two orbits F_0 and F_1 of size $\frac{|X|-1}{2}$, such that $\Delta(x, x) \in F_0$ for $x \neq 0$.

The map ω can not decompose the set $\Delta_0 \cup \Delta^f$ by Lemma 5.10 (1). If ω decomposes $F_0 \cup \Delta_0$ and $\Delta^f \cup F_1$ separately (or decomposes $\Delta^f \cup F_0$ and $\Delta_0 \cup F_1$ separately), since $\omega(\Delta(x, 0)) = \Delta(x, 0)$, then p divides $\frac{|X|-1}{2}$ and so p divides $|X| - 1$, contradiction.

Assume that ω decomposes $F_0 \cup \Delta_0 \cup \Delta^f$ and F_1 separately. Then p divides $\frac{|X|-1}{2}$ and so p divides $|X| - 1$, contradiction. Let us assume that ω decomposes $F_1 \cup \Delta_0 \cup \Delta^f$. Then p divides $\frac{|X|-1}{2} + 2 = \frac{|X|+3}{2}$, then $p = 3$. Let us assume that $\omega(\Delta(x, x)) \in F_0$. Then there exists $k, r \in \mathbb{N}$ such that

$$\omega(x, x) = (2x, x) = f^k(\alpha^r(x), \alpha^r(x))$$

Hence k and r satisfy the following equations

$$(17) \quad \begin{cases} 2x = \alpha^r \left(x + \sum_{j=1}^k (-1)^j \alpha^j \left(x - (1 - \alpha)^{-1}(x) \right) \right) \\ x = (1 - \alpha) \alpha^r \left(x + \sum_{j=1}^{k-1} (-1)^j \alpha^j \left(x - (1 - \alpha)^{-1}(x) \right) \right) \end{cases}$$

where we can assume that $k \leq \frac{|X|-3}{2}$. Moreover we have that

$$(18) \quad p(\omega(x, x)) = 2x - \alpha(x) = p(f^k(\alpha^r(x), \alpha^r(x))) = \alpha^r(x)$$

Taking the difference between the two equations of 17 and using the condition 18 we get

$$x = (-1)^k \alpha^{k+1}(x)$$

since $1 - 2\alpha \stackrel{p=3}{=} 1 + \alpha$ is an automorphism for every $n > 1$. If k is even, then $|X| - 1$ divides $k + 1 \leq \frac{|X|-1}{2}$, which implies $|X| \leq 1$, contradiction. If k is odd then $|X| - 1$ divides $2(k + 1)$, then $\frac{|X|-1}{2}$ divides $k + 1$, i.e. $k = -1$ modulo $\frac{|X|-1}{2}$. Then we get

$$f(\omega(x, x)) = (\alpha^r(x), \alpha^r(x))$$

This condition is equivalent to the system

$$\begin{cases} (1 - \alpha)(2x) + \alpha((1 - \alpha)^{-1}(x)) = \alpha^r(x) \\ (1 - \alpha)(2x) = \alpha^r(x) \end{cases}$$

which imply $x = 0$, contradiction. \square

Proposition 7.17. *Let $X = \mathcal{Q}(\mathbb{Z}_2^n, \alpha)$ be a two-transitive quandle with $n \neq 2$, then $H^2(X, S) = \{1\}$.*

Proof. It follows from Proposition 5.12, since $o(\alpha) = 3$ if and only if $n = 2$. \square

Proposition 7.18. *Let X be a connected quandle of size 4. Then $H^2(X, S) = \{[\beta_\sigma], \sigma^2 = 1\}$ where*

$$(19) \quad \beta_\sigma = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & \sigma & \sigma \\ 1 & \sigma & 1 & \sigma \\ 1 & \sigma & \sigma & 1 \end{bmatrix}$$

and $\beta_\sigma \sim \beta_\tau$ if and only if σ and τ are conjugated.

Proof. There is only one isomorphism class of connected quandles of order 4 and a representative is $X = \mathcal{Q}(\mathbb{Z}_2^2, \alpha)$ where $o(\alpha) = 3$. Every non trivial cocycle $\beta \in Z^2(X, S)$ is equivalent to a 0-normalized cocycle of the form 19 where $\sigma^2 = 1$. By Proposition 4.4, β_σ and β_τ are equivalent if and only if σ and τ are conjugated. \square

REFERENCES

- [1] Nicolas Andruskiewitsch, Matias Graa, *From racks to pointed Hopf algebras*, Advances in Mathematics 178 (2), 177–243 (2003).
- [2] Matias Graa, *Indecomposable racks of order p^2* , Beitrge zur Algebra und Geometrie. Contributions to Algebra and Geometry 45 (2004), no. 2, 665–676.
- [3] Michael Eisermann, *Quandle coverings and their Galois correspondence*, Fundamenta Mathematicae 225 (2014), no. 1, 103–168.
- [4] Giuliano Bianco, *On the Transvection Group of a Rack*, PhD thesis (2015).
- [5] David Joyce, *A Classifying invariant of knots, the knot quandle*, Journal of Pure and Applied Algebra 23 (1982) 37–65, North-Holland Publishing Company.
- [6] P. Etingof, R. Guralnik & A. Soloviev, *Indecomposable set-theoretical solutions to the Quantum Yang–Baxter Equation on a set with prime number of elements*, Journal of Algebra 242 (2001), 709–719.
- [7] Premysl Jedlicka, Agata Pilitowska, David Stanovsky, Anna Zamojska-Dzienio, *Structure of Medial Quandles*, Journal of Algebra 443 (2015), 300–334.

- [8] Ivan I. Deriyenko, *On middle translations of nite quasigroups*, Quasigroups and Related Systems 16 (2008), 17–24.
- [9] L.Vendramin, *Doubly Transitive Group and Quandles*, accepted for publication in J. Math. Soc. Japan.
- [10] Hulpke A., Stanovsky D., Vojtechovsky P., *Connected quandles and transitive groups*, Journal of Pure and Applied Algebra 220 (2016), no. 2, 735–758
- [11] Thompson, John G., *Normal p -complements for finite groups*, Mathematische Zeitschrift, 72 (1960), 332–354

E-mail address, Marco Bonatto: `bntmrc1@unife.it`